U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

October 5, 2017

BY CM/ECF

The Honorable Denise L. Cote
United States District Judge
Southern District of New York
Daniel Patrick Moynihan United States Courthouse
500 Pearl Street
New York, NY 10007

Re: *United States v. David W. Kent*, 16 Cr. 385 (DLC)

Dear Judge Cote:

The Government submits the following addendum to its sentencing submission to discuss the process it used to estimate the loss amount, restitution, and forfeiture amounts in this case.

I. Factual Background

As described in the Presentence Investigation Report ("PSR"), the defendant engaged in two sets of network intrusions into a members database for a professional networking website in the oil and gas industry ("Website-1") that belonged to a company located in New York ("Victim-1"). During these hacks, the defendant accessed approximately 796,000 accounts, which corresponded with approximately 586,560 unique email addresses. (PSR ¶ 45). The defendant intended to invite these Website-1 users to join OilPro.com, a website that the defendant created to compete with Website-1 (PSR ¶¶ 27-30, 35, 45-46). On December 19, 2016, the defendant pleaded guilty pursuant to a plea agreement that included the following stipulations: (1) a loss amount that exceeded $1,500,000 but was less than $3,500,000; (2) a restitution amount of $3,292,800; and (3) a forfeiture amount of $2,932,800.

II. Data Points for Estimating Loss Amount

To reasonably estimate the loss amount associated with the unlawfully accessed data, the Government met with representatives of Victim-1, who explained that Website-1 does not sell copies of its members data in bulk to anyone, and certainly not to its competitors. In other words, there is no well-established market value or price for the data that was unlawfully accessed. Rather, Website-1 offers paid subscriptions to the Website-1 members database to employers and recruiters that provided limited access to the Website-1 members data. For example a one-month subscription to the Website-1 members database includes the ability to view 200 resumes per month and costs $990, or approximately $5/resume. For this reason, Victim-1 proposed to estimate

the value of the stolen data by using the amount of marketing funds that Victim-1 spent to obtain the 586,560 members that were affected by the network intrusions. Using this methodology, Victim-1 believed that a loss amount of approximately $12.8 million was a reasonable estimate if using the average amount of money spent by Victim-1 in marketing costs to obtain a new member. Alternatively, Victim-1 proposed that a loss amount of approximately $44.5 million was an appropriate estimate by multiplying the amount of job applications generated by the 586,560 members affected by the network intrusions and the average marketing costs per generated job application. Ultimately, however, the Government believed that these loss amount formulas--which focused on the amount of money Victim-1 spent to increase Website-1's membership--overstated the attempted loss to Victim-1. Instead, the Government believed that a reasonable loss amount would estimate the fair market value of the data that was stolen--that is, the price that Victim-1 would ask for if it were willing to sell a copy of the data to one of its competitors.

The Government then sought to obtain data points regarding the market value of the stolen data. First, the defendant sold Website-1 to Victim-1 for $51.7 million in 2010. Shortly after the acquisition, an accounting firm was hired to do an independent valuation of the company, which valued the Website-1 members database (containing approximately 900,000 active users)[1] at $6 million, based on the average of two methods: (1) multiplying the average cost of acquiring a unique visitor times the average number of unique visitors to Website-1; and (2) multiplying the cost to obtain a job applicant times the number of applicants that Website-1 could expect from the number of registered seekers in its members database. Second, Victim-1 purchased another professional networking website in the oil and gas industry ("Website-2") for approximately $26 million in 2014. An accounting firm was also hired to do an independent valuation of the company, which valued the Website-2 members database (containing approximately 498,000 active users) at $3.2 million, which was based on a formula that used the amount of money spent annually to maintain and acquire new members for the database. These data points suggested that a ceiling for the value of the stolen data was $6 million. In other words, if Victim-1 paid $6 million for *exclusive* access to Website-1 data associated with 900,000 active users, the market value for a *copy* of this data would likely be sold for less than that amount.

Next, the Government also looked to other transactions (not involving Victim-1) for sales of similar quantities of data in the realm of professional networking websites for the oil and gas industry. The defendant provided to the Government several examples of such transactions, including but not limited to: (1) a sale of approximately 400,000 resumes between two competing professional networking websites in the oil and gas industry for approximately 37 cents per resume; and (2) a sale of approximately 425,000 resumes from a recruiting company to a professional networking website for approximately 20 cents per resume. These sales, however, did not involve Website-1, which is well-known in the industry as the leading professional networking website, which does not sell bulk quantities of resumes to its competitors for this reason. This is also borne out in the prices of subscriptions to Website-1, as the prices to obtain a subscription with Website-1 are reportedly more expensive than subscriptions with competitors. As a result, the Government believed that the lower limit for the value of the stolen data was

[1] An "active user" is defined as a user that added or updated their resume in the last two years. Victim-1 informed the Government that all of the members affected by the defendant's actions were active users.

approximately 37 cents per resume, which would result in a loss amount of approximately $217,000.

Finally, the Government also identified a transaction from October 2013 in which the defendant obtained a list of approximately 140,000 member profiles from a recruitment company and offered to pay $5 for every member that created an OilPro profile. This price of $5/user was generally consistent with the price of a Website-1 subscription for 200 resumes per month at the price of $990. The price of $5/user also resulted in an estimated loss amount of approximately $2,932,800 ($5/user x 586,560 users), which is roughly halfway between the lower bound of $217,000 and the upper bound of $6 million. For this reason, the parties agreed to and stipulated to a forfeiture amount of $2,932,800--an estimate of the market value of the data that was unlawfully accessed and copied.

Next, the Government asked Victim-1 for information regarding the costs associated with remediation and investigation of the offense, specifically excluding any time spent coordinating or providing assistance to law enforcement. *See* Application Note 3, Subsection (A)(v)(III) to U.S.S.G. § 2B1.1 (explaining that actual loss includes response costs, damage assessments, and restoration costs for offenses under 18 U.S.C. § 1030); 18 U.S.C. § 3663A(b)(4) (requiring restitution to victims for "other expenses related to participation in the investigation or prosecution of the offense"). Based on this request, Victim-1 informed the Government that its remediation and investigation costs amounted to approximately $360,000. This figure is based on approximately (1) 620 hours spent by technology-related employees at Webiste-1 and Victim-1, 400 hours spent by in-house legal employees at Victim-1, and 180 hours spent by executive and management employees, which amounts to an estimated cost of approximately $260,000; (2) approximately $65,000 on outside technology investigators; and (3) approximately $35,000 spent on outside legal counsel. Adding these reported remediation costs to the estimated value of the stolen data, the Government proposed a restitution amount of $2,932,800 + $360,000 = $3,292.800. Similarly, the Government proposed a stipulation that the total loss amount exceeded $1,500,000 but was less than $3,500,000, pursuant to U.S.S.G. § 2B1.1(b)(1)(I). Pursuant to the plea agreement, the defendant stipulated to these amounts.

III. Conclusion

For the reasons set forth above, the Government respectfully believes that the Court should adopt the stipulations in the plea agreement, which include: (1) a loss amount that exceeded $1,500,000 but was less than $3,500,000; (2) a restitution amount of $3,292,800; and (3) a forfeiture amount of $2,932,800. The Government believes that these figures represent a reasonable estimate of the relevant loss amount, restitution amount, and forfeiture amount.

Respectfully submitted,

JOON H. KIM
Acting United States Attorney

By: /s/ Sidhardha Kamaraju/Andrew K. Chan
Sidhardha Kamaraju/Andrew K. Chan
Assistant United States Attorneys
(212) 637-6523 / 1072

cc: Dan Cogdell, Esq. and David Spears, Esq.